UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/392,938	09/09/1999	ROBERT B. TACKMAN	99-1852	2037

7590 12/03/2003

JENNIFER M STEC
DAIMLERCHRYSLER INTELLECTUAL
CAPITOL CORPORATION
CIMS 483 02 19 800 CHRYSLER DRIVE EAST
AUBURN HILLS, MI 483262757

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2172	4

DATE MAILED: 12/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/392,938	TACKMAN ET AL.	
	Examiner	Art Unit	
	Thanhnga Truong	2172	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 1999* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1 through 20 rejected under 35 U.S.C. 102(e) as being anticipated by Rowney (US 5,987,140).

a. Referring to claim 1:

i. Rowney teaches:

(1) a server processing unit and a server memory device electrically coupled to the server processing unit **[i.e., a workstation having a central processing unit, such as a microprocessor, and a number of other units (including a Random Access Memory (RAM) and Read Only Memory(ROM)) interconnected via a system bus (column 4, line 1-10)]**,

(2) a client processing unit and a client memory device electrically coupled to the client processing unit **[i.e., a personal computer having a central processing unit, such as a microprocessor, and a number of other units (including a Random Access Memory (RAM) and Read Only Memory(ROM)) interconnected via a system bus (column 4, line 1-10)]**,

(3) a server program module, stored in the server memory device, for providing instructions to the server processing unit **[i.e., the workstation typically has installed an operating system such as the IBM OS/2 operating system or UNIX operating system (column 4, line 15-20)]**,

(4) a client program module, stored in the client memory device, for providing instructions to the client processing unit **[i.e., the personal computer includes an operating system such as the Microsoft Windows Operating System (OS) (column 4, 15-17)]**, and

(5) a communication medium, communicatively coupling the server processing unit and the client processing unit **[i.e., secure transmission of data is provided between a plurality of computer systems over a public communication systems, such as the Internet (column 2, line 60-62)]**;

(6) the client processing unit, responsive to the instruction of the client program module and the server processing unit, responsive to the instructions of the server program module **[figure 2]**, being operative to:

(a) authorize access to the system **[i.e., customer computer system transmits a client certificate to enable customer computer system to authenticate the identity of customer computer system (column 11, line 30-34)]**;

(b) generate at least one electronic document **[i.e., customer computer system initiates communication by sending "client hello" message to the merchant computer system (column 10, line 31-33)]**;

(c) prevent the creation of fraudulent versions of the electronic document **[i.e., by using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications between the two computer systems, which may thereafter engage in secure communications "to prevent the creation of fraudulent versions of the electronic document" is considered with less risk of interception by third parties (column 11, line 53-58)]**;

(d) allow electronic signatures to be associated with the electronic document, thereby generating an electronic agreement **[i.e., provide a server key exchange message, which may be used by a client to decrypt message, that is, "electronic signatures to be associated with the electronic document" sent by the server (column 11, line 20-24). Furthermore, Rowney's**

invention utilizes HyperText Markup Language (HTML) to implement documents on the Internet together with a general-purpose secure communication protocol, that is, electronic argreement, for a transport medium between the client and the merchant (column 8, lines 57-60)]; and

(e) maintain an authoritative copy of the electronic document in the server memory device of the server processing unit **[i.e., merchant computer system stores capture response, that is, "maintain an authoritative copy of the electronic document", for later use in by legacy system accounting program, e.g. to perform reconciliation between the merchant operating merchant computer system and the financial institution from whom payment was requested, thereby completing the transaction (column 20, line 3-8)].**

b. Referring to claim 2 which depends on claim 1:

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving access information from the input device **[i.e., server certificate enables customer computer system to authenticate the identity of merchant computer system (column 11, line 14-17)]**,

(b) transmitting the access information to the server over the communication medium **[i.e., customer computer system transmits client certificate to the merchant computer system enabling the server to authenticate the identity of customer computer system (column 11, line 30-34)]**, and

(c) receiving an authorization indicator from the server processing unit over the communication medium **[i.e., server hello message includes an indicator of the cryptographic algorithms selected from among the algorithms specified by client hello message, which will be used in further encrypted communications (column 11, line 10-13)]**; and

(3) the server processing unit **[i.e., Figure 1A]**

(a) receiving the access information from the client processing unit over the communications medium **[i.e., message communicated by customer computer system to merchant computer system may be of goods and services to be ordered and payment information(column 11, line 59-64)]**,

(b) verifying that the access information qualifies for granting access to the system **[i.e., merchant computer system processes the purchase request from customer in accordance with the authorization response, determining whether a request should be granted or denied (column 16, line 13-20)]**, and

(c) transmitting an authorized indicator to the client processing unit over the communication medium **[i.e., server hello message includes an indicator of the cryptographic algorithms selected from among the algorithms specified by client hello message, which will be used in further encrypted communications (column 11, line 10-13)];**

c. Referring to claim 3 which depends on claim 1:

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving pertinent information from the input **[i.e., server hello message allowing client to connect with merchant computer system (column 10, line 61-62)]**, and

(b) integrating the pertinent information into an electronic template **[i.e., combining the server hello message and client related message sent by customer computer system or client wherein the message that specify goods or services to be ordered and payment information (column 11, line 59-63)]**;.

d. Referring to claim 4 which depends on claim 3:

i. Rowney further teaches:

(1) receiving a complete indicator from the input device, the complete indicator indicating that no additional pertinent information will be received by the client processing unit **[i.e., merchant computer system provides server**

certificate or server key exchange message and as well as server hello done message (column 11, line 25-28)], and

(2) merging the pertinent information and the predefined document information to generate the electronic document conforming to the predefined document format **[i.e., combining the server message and client related message sent by customer computer system or client wherein the message that specify goods or services to be ordered and payment information (column 11, line 59-63)]**;

e. Referring to claim 5:

i. Rowney further teaches:

(1) an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic document by the client processing unit, in response to generating the electronic document, rejecting any attempts to modify the electronic document **[i.e., payment gateway computer system verifies merchant computer system's encryption and signature public key certificates by calculating a message over the content of said combined authorization request, then decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system. If the two messages are the same, the digital signature is validated, otherwise, payment gateway computer system rejects the authorization request (column 14, line 4-14)]**.

f. Referring to claim 6:

i. Rowney further teaches:

(1) an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic document by the client processing unit, in response to generating the electronic document, encrypting the electronic document and generating a signature key based at least in part on the contents of the electronic document **[i.e., the merchant computer systems**

combines basic authorization request, a copy of its encryption public key certificate, and a copy of its signature public key certificate. It further calculates a digital signature for the combined contents/messages of the combine block comprising basic authorization request. The merchant computer system calculates digital signature by first calculating a "message digest" based upon the contents of the combined basic authorization request. Message digest help verify that a message has not been altered because altering the message would change the digest. The message digest is then encrypted using the merchant computer system's digital signature private key (column 12, line 43-65)].

g. Referring to claim 7:

i. Rowney further teaches:

(1) the client processing unit **[i.e. Figure 1A]**

(a) in response to generating the electronic document, encrypting the electronic document **[i.e., the message digest is then encrypted using the merchant computer system's digital signature private key (column 12, line 63-65)]**, and

(b) in response to an attempt to modify the electronic document, rendering the electronic document invalid **[i.e., a message digest help verify that a message has not been altered because altering the message would change the digest (column 12, line 60-63), and payment gateway computer system verifies merchant computer system's encryption and signature public key certificates by calculating a message over the content of said combined authorization request, then decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system. If the two messages are the same, the digital signature is validated, otherwise, payment gateway computer system rejects the authorization request (column 14, line 4-14)].**

h. Referring to claim 8:

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving at least one signature input from the input device **[i.e., payment gateway computer system receives and verifies merchant computer system's encryption and signature public key certificates, and as well as digital signature (column 13, line 54-58)]**,

(b) creating a signature file containing the signature input **[i.e., payment gateway computer system creates a basic authorization response, and a copy of its signature public key certificate (column 14, line 25-35)]** , and

(c) encrypting the signature file using an encryption key that is based at least in part on the contents of the electronic document **[i.e., payment computer system calculates a digital signature by first calculating a message digest based on the contents of the combined basic authorization response and the signature public key certificate. The message digest is then encrypted using the merchant computer system's digital signature private key (column 14, line 40-50)].**

i. Referring to claim 9:

i. Rowney further teaches:

(1) the client processing unit **[i.e., Figure 1A]**

(a) receiving a submit indicator from the input device **[i.e., in order to obtain payment from the customer, the merchant must supply/submit payment information to the bank or other payment gateway responsible for the payment method (column 11, line 65-68)]**, and

(b) in response to receiving the submit indicator, transmitting the electronic document and the electronic signatures associated with the electronic document to the server processing unit over the communication medium **[i.e., the merchant computer systems transmits a payment authorization request by combining basic authorization request, a copy of its encryption public key certificate, and a copy of its signature public key certificate. It further calculates a digital signature for the combined contents/messages of the combined block**

comprising basic authorization request, then transmits over the communication network (column 12, line 43-53)]; and

(2) the server processing unit **[i.e., Figure 1A]**

(a) receiving the electronic document and the electronic signatures **[i.e., payment gateway computer system receives a payment authorization request and verifies merchant computer system's encryption and signature public key certificates, and as well as digital signature (column 13, line 54-58)]**,

(b) preventing any modifications to the electronic document and the signature file **[i.e., then decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system. If the two messages are the same, the digital signature is validated, otherwise, payment gateway computer system rejects the authorization request (column 14, line 4-14)]**, and

(c) providing an unauthorized copy indicator on any electronic and hard copies of the electronic document, the unauthorized copy indicator indicating that the electronic and hard copies of the electronic document are not the authoritative copy of the electronic document **[i.e., payment gateway computer system contacts the appropriate financial institution using a secure means, e.g., a direct-dial modem-to-modem connection, or a proprietary internal network that is not accessible to third parties, and using prior art means, obtains a response indicating whether the requested payment is authorized (column 14, line 16-24)].**

j. Referring to claim 10:

i. Rowney teaches:

(1) receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic document **[i.e., payment gateway system receives and processes a payment authorization request from the merchant (column 12, line 15-20];**

(2) in response to receiving a complete indicator from the input source, the complete indicator indicating that the received subset of input information is complete, generating an electronic document by merging the subset of input information with a document template **[i.e., the gateway system then generates the basic authorization response and combines it with a copy of its signature public key certificate. The data request is then encrypted using the merchant computer system's digital signature private key and transmits it back to the merchant computer system (column 14, line 25-50)];**

(3) receiving a set of electronic signatures from the input source, whereby up receiving the set of electronic signatures, the electronic document is considered an electronic agreement **[i.e., the merchant computer system then decrypts digital signature which received from payment gateway computer system to obtain a copy of the equivalent data request. If the two data requests are the same, the digital signature is validated (column 16, line 3-8)]**; and

(4) in response to receiving a submit indicator, storing the electronic agreement within an access restricted computer system, the stored electronic agreement constituting an authoritative copy of the electronic agreement **[i.e., the merchant computer system stores capture response, that is, electronic agreement, for later use in by legacy system accounting program, in which to perform reconciliation between the merchant and the financial institution, thereby completing the transaction (colulmn 20, line 3-8). Furthermore, Rowney's invention utilizes HyperText Markup Language (HTML) to implement documents on the Internet together with a general-purpose secure communication protocol, that is, electronic argreement, for a transport medium between the client and the merchant (column 8, lines 57-60)].**

k. Referring to claim 11 which depends on claim 10:

i. Rowney further teaches:

(1) after the generating step, the step of providing a signature indicator to the input source, the signature indicator indicating that the generating step is complete and that the electronic documents requires the input of the

set of electronic signatures **[i.e., payment gateway computer system validates merchant digital signature (column 14, line 1-2)]**.

l. Referring to claim 12 which depends on claim 11:

i. Rowney further teaches:

(1) the step of encrypting the electronic document **[i.e., the payment gateway computer system calculates digital signature by first calculating a message digest based on the contents of the combined basic authorization response and signature public key certificate. The message digest is then encrypted using the merchant computer system's digital signature private key (column 14, line 25-50)]**;

m. Referring to claim 13 which depends on claim 12:

i. Rowney further teaches:

(1) the step of preventing the electronic document from being modified **[i.e., the payment gateway computer system uses a message digest method to detect if the contents have been altered. The message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. It helps verify that a message has not been altered because altering the message would change the digest (column 12, line 55-65)]**.

n. Referring to claim 14 which depends on claim 10:

i. Rowney further teaches:

(1) prior to the storing step,

(a) the step of encrypting the set of electronic signatures using an encryption key **[i.e., payment gateway computer system encrypts combined block using random encryption key RK-1 to form encrypted combined block. It then encrypts random encryption key RK-1 using the public key of merchant computer system to form encrypted random key RK (column 14, line 56-68)]**,

(b) the encryption key being based, at least in part, on the contents of the electronic document **[i.e., the payment gateway computer system calculates digital signature by first calculating a message**

digest based on the contents of the combined basic authorization response and signature public key certificate. The message digest is then encrypted using the merchant computer system's digital signature private key (column 14, line 25-50)], whereby

(c) if the contents of the electronic document are modified, the electronic signatures and the electronic agreement will be invalid **[i.e., after decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system, if the two messages are the same, the digital signature is validated. Otherwise, payment gateway computer system rejects the authorization request, and the electronic agreement is counterfeit (column 14, line 4-14)].**

o. Referring to claim 15 which depends on claim 10:

i. Rowney further teaches:

(1) the step of providing an indicator that the set of electronic signatures has been received and that the electronic agreement is complete **[i.e., payment gateway computer system receives a payment authorization request and verifies merchant computer system's encryption and signature public key certificates, and as well as digital signature (column 13, line 54-58)].**

p. Referring to claim 16:

i. Rowney teaches:

(1) a client device receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic document and a set of signatures necessary to make the electronic document a binding agreement **[i.e., payment gateway computer system receives and processes a payment authorization request from the merchant, generates a payment authorization response, that is, electronic agreement, whereby the authorization request combines with a copy of its encryption public key certificates and a copy of its signature public key certificate (column 12, line 15-20 and line 43-48)]**;

(2) a client device encrypting the electronic document using a first key and the set of signatures using a second key, the second key being based at least in part on the contents of the electronic document, whereby any modifications to the electronic document would result in invalidating the set of signatures **[i.e., the payment gateway computer system uses its private key to encrypted random key contained within received merchant authorization request, thereby decrypting it and obtaining a cleartext version of random key RK-0, the gateway system then applies random key RK-0 to encrypted combined block, thereby decrypting it and obtaining a cleartext version of combined block. Finally, the gateway system decrypts digital signature to obtain a copy of the equivalent data request. If the two data requests are the same, the digital signature is validated. If the validation fails, the gateway computer system rejects the authorization request (column 13, line 45-53; and column 14, line 8-14)]**;

(3) a client device transferring the encrypted electronic document and the encrypted set of signature to a server device over a communication medium, the server device being access restricted, the stored electronic document and set of signature constituting the only authoritative copy of the electronic agreement **[i.e., the merchant computer system stores capture response, that is electronic agreement, for later use in by legacy system accounting program, in which to perform reconciliation between the merchant and the financial institution, thereby completing the transaction (column 20, line 3-8). The system of the present invention permits immediate deployment of a secure payment technology architecture such as the SET architecture without first establishing a public-key encryption, that is "access restricted", infrastructure for use by consumers (column 20, lines 9-12)]**.

q. Referring to claim 17:

i. Rowney teaches:

(1) a client processing uint **[i.e., Figure 1A]**;

(2) a client memory device **[i.e., Figure 1A, a Random Access Memory (RAM) 14 and Read Only Memory (ROM) 16]**,

(a) a display device **[i.e., Figure 1A, display device (38)]** and

(b) an input device **[i.e., Figure 1A, a keyboard (24), a microphone (32), a mouse (26), and a speaker (28)]**

(3) a client program module, stored in the client memory, for proving instructions to the client processing unit **[i.e., the personal computer or workstation typically has resident an operating system such as the Microsoft Windows Operating System(OS), the IBM OS/2 operating system, etc.. (column 4, line 14-16)]**;

(4) a communication medium, communicatively coupling the client system to the electronic document system **[i.e., Figure 1A, communication adapter (34) for connecting the personal computer or workstation to a communication network, which operates with a secure communication protocol such as the SSL protocol (column 4, line 10-13 and column 10, line 7-8)]**

(5) the client processing unit **[i.e., Figure 1A]**, responsive to the instructions of the client program module, being operative to:

(6) authorize access to the electronic document system by **[i.e., customer computer system transmits a client certificate to enable merchant computer system to authenticate the identity of customer computer system (column 11, line 30-34)]**

(a) receiving access information from the input device **[i.e., server certificate enables customer computer system to authenticate the identity of merchant computer system (column 11, line 14-17)]**,

(b) transmitting the access information to the server over the communication medium **[i.e., customer computer system transmit client certificate to the merchant computer system enabling the server to authenticate the identity of customer computer system (column 11, line 30-34)]**, and

(c) receiving an authorization indicator from the server processing unit over the communication medium **[i.e., server hello message includes an indicator of the cryptographic algorithms selected from among the algorithms specified by client hello message, which will be used in further encrypted communications (column 11, line 10-13)]**;

(7) generate at least one electronic document **[i.e., customer computer system initiates communication by sending "client hello" message to the merchant computer system (column 10, line 31-33)]**;

(8) prevent the creation of fraudulent versions of the electronic document **[i.e., by using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications between the two computer systems, which may thereafter engage in secure communications "to prevent the creation of fraudulent versions of the electronic document" is considered with less risk of interception by third parties (column 11, line 53-58)]**;

(9) allow electronic signatures to be associated with the electronic document, thereby generating an electronic agreement **[i.e., receiving a server key exchange message, which may be used by a client to decrypt further message, that is, "electronic signatures to be associated with the electronic document" sent by the server (column 11, line 20-24). Furthermore, Rowney's invention utilizes HyperText Markup Language (HTML) to implement documents on the Internet together with a general-purpose secure communication protocol,**

that is, electronic argreement, for a transport medium between the client and the merchant (column 8, lines 57-60)];

(a) receiving a set of signatures from the input device **[i.e., receiving a server key exchange message, which may be used by a client to decrypt further message, that includes "a set of signatures" sent by the server (column 11, line 20-24)]**

(b) creating at least one signature file containing the set of signature **[i.e., establishing a client key exchange message, that is "creating at least one signature file containing the set of signature" which may be used by the server to decrypt message sent by the client (column 11, line 40-44)]** , and

(c) encrypting the signature using a encryption key that is based at least in part on the contents of the electronic document **[i.e., using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications between the two computer systems (column 11, line 53-55)]**; and

(10) transfer the electronic document and the encrypted signature file to the server over the communication medium **[i.e., client transmit a complete message, that is "the electronic document" to the server by including a set of encryption keys, which may thereafter engage in secure communications with less risk of interception by third parties (column 11, line 45-58)];**

r. Referring to claim 18 which depends on:

i. Rowney further teaches:

(1) receiving pertinent information from the input device **[i.e., server hello message allowing client to connect with merchant computer system (column 10, line 61-62)],**; and

(2) merging the pertinent information with predefined document information to generate an electronic document conforming to a predefined document format **[i.e., combining the server message and client hello message sent by customer computer system or client wherein the message that specify goods or services to be ordered and payment information (column 11, line 59-63)].**

s. Referring to claim 19 which depends on claim 17:

i. Rowney further teaches:

(1) the client processing unit is operative to prevent the creation of fraudulent versions of the electronic document by, after generating the electronic document, encrypting the electronic document and rejecting any attempts to enter additional pertinent information **[i.e., the payment gateway computer system uses a message digest method to detect if the contents have been altered. The message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. It helps verify that a message has not been altered because altering the message would change the digest. The message digest is then encrypted using the merchant computer system's digital signature private key (column 12, line 55-65)].**

t. Referring to claim 20 which depends on claim 17:

i. Rowney further teaches:

(1) detecting an attempt to modify the electronic document **[i.e., the payment gateway computer system uses a message digest method to detect if the contents have been altered. The message digest is the fixed-length result that is generated when a variable length message is fed into a one-way hashing function. It helps verify that a message has not been altered because altering the message would change the digest (column 12, line 55-63)**, and

(2) in response to detecting an attempt, rendering the electronic document invalid **[i.e., after decrypting digital signature to obtain a copy of the exact message calculated by the merchant computer system, if the two**

messages are the same, the digital signature is validated. Otherwise, payment gateway computer system rejects the authorization request, and the electronic document is counterfeit (column 14, line 4-14)].

Response to Argument

3. Applicant's arguments filed October 23, 2003 have been fully considered but they are not persuasive.

Applicant argues that:

"by distinction, Rowney at al. is concerned with data encryption for secure transmission of authorization requests for credit, not with the generation and maintenance of electronic agreements and electronic signatures as called for in Applicants' claims."

Examiner maintains that:

Rowney's invention utilizes HyperText Markup Language (HTML) to implement documents on the Internet together with a general-purpose secure communication protocol, that is, electronic argreement, for a transport medium between the client and the merchant (column 8, lines 57-60). Figure 3 in Rowney depicts an overview of the method of securely supplying payment information to a payment gateway in order to obtain payment authorization. In function block 310, merchant computer system 130 generates a payment authorization request 315 and transmits it to payment gateway computer system 140. In function block 330, payment gateway system 140 processes the payment authorization request, generates a payment authorization response 325 and transmits it to merchant computer system 130 (column 12, lines 12-20). Figure 14 of Rowney shows In function block 1450, merchant computer system 130 stores capture response, that is maintained in the system, for later use in by legacy system accounting programs, e.g. to perform reconciliation between the merchant operating merchant computer system 130 and the financial institution from whom payment was requested, thereby completing the transaction (column 20, lines 3-8).

Applicant also argues that:

"Rowney et al. does not teach Applicants' prevention of creation of fraudulent versions of an agreement. Rather, Rowney et al. is concerned with message transmission encryption (see Col. 11, lines 53-58)."

Examiner maintains that:

Rowney teaches by using a set of encryption keys to communicate with each other where the keys may be used to decrypt further communications between the two computer systems, which may thereafter engage in secure communications "to prevent the creation of fraudulent versions of the electronic document" is considered with less risk of interception by third parties (column 11, line 53-58).

Applicant also argues that:

"Rowney et al. is devoid of any suggestion of Applicants' "electronic signatures" as that term is used in the instant case (see Applicants' specification beginning at line 22 of page 17 in conjunction with Fig. 10)."

Examiner believes that:

In function block 1020, merchant computer system 130 combines basic capture request 1110, a copy of its encryption public key certificate 1115 and a copy of its signature public key certificate 1120. Merchant computer system 130 calculates a digital signature, that is "electronic signature", 1125 for the combined contents of the combined block 1130 comprising basic capture request 1110, the encryption public key certificate 1115 and the signature public key certificate 1120, and appends it to the combination of the combined basic capture request 1110, the encryption public key certificate 1115 and the signature public key certificate 1120. The merchant computer system calculates digital signature 1125 by first calculating a message digest over the contents of the combined basic capture request 1110, the encryption public key certificate 1115 and the signature public key certificate 1120. The message digest is then encrypted using the merchant computer system's 130 digital signature private key, thus forming a digital signature. (column 16, lines 50-67).

Applicant also argues that:

"Rowney's random capture token 770 generated by payment Gateway Computer 140 is cited by the Examiner as corresponding to Applicants' allowing electronic signatures to be associated with the electronic document. However, token 770 is used to associate a payment capture request with a payment authorization request being processed-not to indicate that an electronic agreement has been electronically signed."

Examiner maintains that:

Figure 3 in Rowney depicts an overview of the method of securely supplying payment information to a payment gateway in order to obtain payment authorization. In function block 310, merchant computer system 130 generates a payment authorization request 315 and transmits it to payment gateway computer system 140. In function block 330, payment gateway system 140 processes the payment authorization request, generates a payment authorization response 325, that is confirming of digital signature signed, and transmits it to merchant computer system 130 (column 12, lines 12-20).

Applicant also argues that:

"Additionally, Rowney et al. does not teach, claim or even suggest Applicants' maintenance of an authoritative copy of the electronic agreement at the server."

Examiner maintains that:

Figure 14 in Rowney shows In function block 1450, merchant computer system 130 stores capture response, that is maintained in the system, for later use in by legacy system accounting programs, e.g. to perform reconciliation between the merchant operating merchant computer system 130 and the financial institution from whom payment was requested, thereby completing the transaction (column 20, lines 3-8).

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See

MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone numbers for the organization where this application or proceeding is assigned are 703-872-9306 for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
December 1, 2003

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100